UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,712	03/09/2004	Eric Sprunk	D03043	2860

43471   7590   04/03/2008

Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196

EXAMINER
HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
04/03/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.Schaumburg@motorola.com
APT099@motorola.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/796,712	SPRUNK ET AL.
	Examiner	**Art Unit**	
	MATTHEW T. HENNING	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *3/9/04, 3/14/2006*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

1   This action is in response to the communication filed on 3/9/2004.

2   **DETAILED ACTION**

3   Claims 1-43 have been examined.

4   *Title*

5   The title of the invention is acceptable.

6   *Information Disclosure Statement*

7   The information disclosure statement(s) (IDS) submitted on 3/14/2006, and 3/9/2004 are

8   in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the

9   information disclosure statements.

10   *Drawings*

11   The drawings filed on 1/17/2006 are acceptable for examination proceedings.

12   *Specification*

13   The disclosure is objected to because of the following informalities: Paragraphs 0002 and

14   0003 appear to have been mistakenly included and should therefore be removed.

15   Appropriate correction is required.

16   ***Claim Objections***

17   Claim 34 is objected to because of the following informalities: Claim 34 lacks a

18   terminating period. Appropriate correction is required.

19

20   ***Claim Rejections - 35 USC § 102***

21   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

22   basis for the rejections under this section made in this Office action:

1   *A person shall be entitled to a patent unless –*

2   *(b) the invention was patented or described in a printed publication in this or a foreign*
3 *country or in public use or on sale in this country, more than one year prior to the date of*
4 *application for patent in the United States.*
5
6   Claims 1, 3, 5-14, 16-23, 31-37, and 40-43 are rejected under 35 U.S.C. 102(b) as being

7 anticipated by Fischer (US Patent Number 5,475,826).

8   Regarding claims 1 and 23, Fischer disclosed a method of authenticating a set of N

9 information blocks (See Fig. 2), said method comprising: obtaining an initial root key for a set of

10 data comprised of a plurality of blocks of data, said root key operable for authenticating said set

11 of data (See Col. 9 Paragraph 2); calculating hash keys for said plurality of blocks of data so that

12 each of said hash keys corresponds to only one of said blocks of data and so that each of said

13 blocks of data corresponds to only one of said hash keys (See Col. 9 Paragraph 4); storing said

14 hash keys for said plurality of blocks of data (See Col. 9 Paragraph 4 wherein it was inherent that

15 the hashes were stored at least temporarily); altering one of said blocks of data so as to form a

16 revised block of data (See Col. 9 Line 64 - Col. 10 Line 3); calculating a second hash key for

17 said revised block of data, wherein said revised block of data immediately prior to being revised

18 corresponds to a first hash key and wherein said first hash key is one of said hash keys for said

19 plurality of blocks of data (See Col. 10 Paragraph 4); utilizing said stored hash keys, including

20 said first hash key, to calculate a check root key (See Col. 9 Paragraph 4) while utilizing said

21 stored hash keys and said second hash key substituted in place of said first hash key to calculate

22 a new root key (See Col. 10 Lines 54-60); comparing said check root key with said initial root

23 key (See Col. 10 Line 66 - Col. 11 Line 1); accepting said new root key if said check root key

24 matches said initial root key (See Col. 11 Paragraph 1).

1

2   Regarding claim 3, Fischer disclosed calculating said revised hash value while

3   calculating said check hash value comprises: hashing said altered block of data so as to obtain a

4   first hashing result; storing said first hashing result in a processor; and then hashing the

5   corresponding unaltered block of data so as to obtain a second hashing result (See Fischer Col. 9

6   Paragraph 4 - Col. 10 Paragraph 4).

7   Regarding claim 5, Fischer disclosed that calculating said revised hash value while

8   calculating said check hash value comprises: utilizing a single processor to calculate said revised

9   hash value and to calculate said check hash value (See Fischer Col. 4 Line 31-45).

10   Regarding claim 6, Fischer disclosed performing a linear hash of said set of data by

11   hashing said N blocks of data in sequential order from block 1 to block N (See Fischer Col. 10

12   Lines 45-53).

13   Regarding claim 7, Fischer disclosed hashing each of said N information blocks in said

14   set of N information blocks (See Fischer Col. 10 Lines 45-53).

15   Regarding claim 8, Fischer disclosed storing said initial hash value in a processor (See

16   Fischer Col. 9 Paragraph 2).

17   Regarding claim 9, Fischer disclosed storing a new value for at least part of one of said N

18   information groups (See Fischer Col. 10 Lines 25-53).

19   Regarding claims 10 and 35, Fischer disclosed determining whether said check hash

20   value and said initial hash value are exactly the same (See Fischer Col. 11 Paragraph 1).

1   Regarding claims 11 and 36, Fischer disclosed replacing said initial hash value with said

2   revised hash value (See Fischer Col. 8 Lines 45-50).

3   Regarding claims 12 and 37, Fischer disclosed storing the new revised hash value in the

4   memory area previously occupied by the initial hash value (See Fischer Col. 8 Lines 45-50).

5   Regarding claim 13, Fischer disclosed not accepting said revised hash value as a

6   replacement for said initial hash value if said check hash value does not match said initial hash

7   value (See Fischer Col. 11 Paragraph 1).

8   Regarding claim 14, Fischer disclosed indicating a failure to authenticate (See Fischer

9   Col. 11 Paragraph 1).

10   Regarding claim 16, Fischer disclosed replacing said initial hash value with said revised

11   hash value (See Fischer Col. 7 Line 65 - Col. 8 Line 15 and Col. 8 Line 58 - Col. 11 Line 10 and

12   Fig. 1).

13   Regarding claims 17 and 40, Fischer disclosed receiving as part of an initialization

14   routine a length of a data set to be hashed, wherein said data set is comprised of said N

15   information groups (See Fischer Col. 7 Line 65 - Col. 8 Line 15 and Col. 8 Line 58 - Col. 11

16   Line 10 and Fig. 1).

17   Regarding claim 18, Fischer disclosed padding at least one of said N information groups

18   so that each of said N information groups is of equal length (See Fischer Col. 7 Line 65 - Col. 8

19   Line 15 and Col. 8 Line 58 - Col. 11 Line 10 and Fig. 1).

20   Regarding claims 19 and 42, Fischer disclosed initializing a processor so as to perform a

21   hashing routine (See Fischer Col. 7 Line 65 - Col. 8 Line 15 and Col. 8 Line 58 - Col. 11 Line 10

1   and Fig. 1).

2   Regarding claim 20, Fischer disclosed initializing a hashing routine by entering the

3   length of said set of data (See Fischer Col. 7 Line 65 - Col. 8 Line 15 and Col. 8 Line 58 - Col.

4   11 Line 10 and Fig. 1).

5   Regarding claims 21 and 43, Fischer disclosed dividing the set of data into a plurality of

6   blocks (See Fischer Col. 7 Line 65 - Col. 8 Line 15 and Col. 8 Line 58 - Col. 11 Line 10 and Fig.

7   1).

8   Regarding claims 22 and 41, Fischer disclosed dividing the set of data into a plurality of

9   blocks of data; padding the last block of data so that each of said blocks of data is of equal length

10   (See Fischer Col. 7 Line 65 - Col. 8 Line 15 and Col. 8 Line 58 - Col. 11 Line 10 and Fig. 1).

11   Regarding claim 31, Fischer disclosed encrypting said hash keys for said plurality of

12   blocks; and storing said encrypted hash keys in memory outside of a processor (See Fischer Col.

13   7 Lines 3-14).

14   Regarding claim 32, Fischer disclosed storing said hash keys for said plurality of blocks

15   in a processor (See Fischer Col. 7 Lines 3-14).

16   Regarding claim 33, Fischer disclosed storing said root key inside a processor (See

17   Fischer Fig. 1).

18   Regarding claim 34, Fischer disclosed storing a new value for at least part of one of said

19   information groups (See Fischer Col. 9 Line 64 – Col. 10 Line 3).

20

1   ***Claim Rejections - 35 USC § 103***

2   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

3   obviousness rejections set forth in this Office action:

4   *A patent may not be obtained though the invention is not identically disclosed or*
5   *described as set forth in section 102 of this title, if the differences between the subject matter*
6   *sought to be patented and the prior art are such that the subject matter as a whole would have*
7   *been obvious at the time the invention was made to a person having ordinary skill in the art to*
8   *which said subject matter pertains. Patentability shall not be negatived by the manner in which*
9   *the invention was made.*
10

11   Claims 2 ,4, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over

12   Fischer. While Fischer did not specifically disclose parallel processing, it was well known that

13   processing can be accomplished concurrently in order to save time and therefore would have

14   been obvious to have done so.

15   Claims 15, 28-30, and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable

16   over Fischer, and further in view of Sprunk et al. (US Patent Number 5,754,659) hereinafter

17   referred to as Sprunk.

18   While Fischer disclose a method for updating a hash for a file when a record in the file is

19   altered, Fischer failed to disclose the use of a branch key in the hashing system, or that the

20   system was used for signing digital media rights data.

21   Sprunk teaches an efficient hashing method including the limitations of claims 25-30, and

22   further teaches that the hashing system can be used to sign access right data (See Sprunk Col. 6

23   Line 50 – Col. 11 Line 14).

24   It would have been obvious to the ordinary person skilled in the art at the time of

25   invention to employ the teachings of Sprunk in the signature system Fischer. This would have

1 been obvious because the ordinary person would have been motivated to increase the efficiency

2 of the system.

3   *Conclusion*

4   Claims 1-43 have been rejected.

5   The prior art made of record and not relied upon is considered pertinent to applicant's

6 disclosure.

7   Any inquiry concerning this communication or earlier communications from the

8 examiner should be directed to MATTHEW T. HENNING whose telephone number is

9 (571)272-3790. The examiner can normally be reached on M-F 8-4.

10   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

11 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

12 organization where this application or proceeding is assigned is 571-273-8300.

13   Information regarding the status of an application may be obtained from the Patent

14 Application Information Retrieval (PAIR) system. Status information for published applications

15 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

16 applications is available through Private PAIR only. For more information about the PAIR

17 system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

18 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

19 like assistance from a USPTO Customer Service Representative or access to the automated

20 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

21
22
23   /Matthew T Henning/
24   Examiner, Art Unit 2131

1

2   /Ayaz R. Sheikh/

3   Supervisory Patent Examiner, Art Unit 2131